

BANKU PIKŠĶERĒŠANAS E-PASTI

Pikšķerēšana nozīmē krāpnieciskus e-pastus, kas saņēmēju mudina dalīties ar personas, finansiālu vai drošības informāciju.

KĀ TAS NOTIEK?

Šie e-pasti:

var **izskatīties** līdzīgi tai saziņai, kādu sūta īstas bankas.

atdarinot īstā e-pastā redzamo logo, izkārtojumu un stilu.



prasa lejupielādēt pievienoto failu vai sekot saitei.

veidoti tā, lai radītu steidzamības sajūtu.

KĀ JUMS RĪKOTIES?

- **Regulāri jauniniet programmatūru, pārlūku, antivīrusu, operētājsistēmu.**
- **Esiet īpaši piesardzīgs, ja "bankas" e-pasts no jums pieprasa sensitīvu informāciju (piemēram, jūsu internetbankas konta paroli).**
- **Rūpīgi aplūkojiet e-pastu, salīdziniet adreses ar iepriekš no bankas saņemtajām ziņām. Pārbaudiet gramatikas un valodas kļūdas.**
- **Neatbildiet un aizdomīgo e-pastu, tā vietā pārsūtiet to uz banku pašrocīgi ievadot bankas adresi.**
- **Nesekoiet saitei vai nelejupielādējiet pielikumu, tā vietā ievadiet adresi pārlūkā.**
- **Ja rodas šaubas, pārbaudiet informāciju bankas tīmekļa vietnē vai telefoniski.**



Noziedznieki paļaujas uz cilvēku aizņemtību. Virspusēji novērtējot, viltotie e-pasti izskatās kā īsti.



Uzmanieties izmantojot mobilās iekārtas! Pamanīt pikšķerēšanas mēģinājumu telefonā vai planšētdatorā būs grūtāk.

#CyberScams

